Formal verification of medical user interface software in PVS

Paolo Masci
Queen Mary University of London
(paolo.masci@eecs.qmul.ac.uk)

Joint work with
Paul Jones, Yi Zhang (U.S. Food and Drug Administration – FDA)
Patrick Oladimeji, Harold Thimbleby (Swansea University)
Paul Curzon, Michael Harrison (QMUL)
Insup Lee, Oleg Sokolsky (UPenn)

SSFT14 – May 22nd, 2014

Queen Mary University of London

chi+med making medical devices safer

CHI+MED research project

www.chi-med.ac.uk

Long-term aim: to transform the design and use of medical devices so as to help clinicians avoid and recover from human error

Combining a variety of approaches

- Mathematical analysis of device designs
- Contextual studies in hospitals
- Lab-based experiments
- Understanding manufacturer's context
- Public engagement

UCL · Swansea University Prifysgol Abertawe · Queen Mary University of London · City University London · EPSRC Engineering and Physical Sciences Research Council

Formal verification – key achievements within chi+med

1. User interface software

- Verification of safety requirements provided by regulators
- Verification of interaction design principles (e.g., consistency)

2. Socio-technical systems

- Analysis of contextual study data / field observations
- Analysis of incidents reports

3. Tool support for model-based prototyping

- Validation of models, safety requirements, analysis results

4. Case studies based on real medical devices

- We identified previously undetected defects in medical devices in use in hospitals

Formal verification – key achievements within chi+med

1. User interface software

- Verification of safety requirements provided by regulators
- Verification of interaction design principles (e.g., consistency)

2. Socio-technical systems

- Analysis of contextual study data / field observations
- Analysis of incidents reports

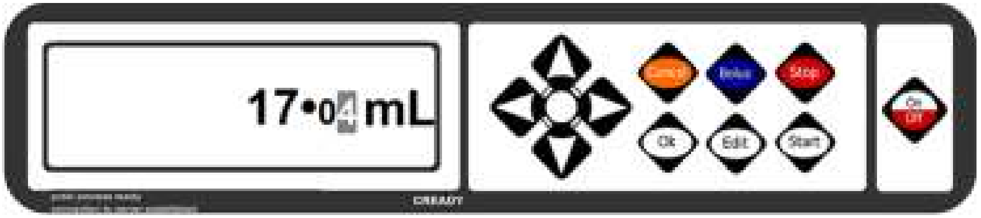
3. Tool support for model-based prototyping

- Validation of models, safety requirements, analysis results

4. Case studies based on real medical devices

- We identified previously undetected defects in medical devices in use in hospitals

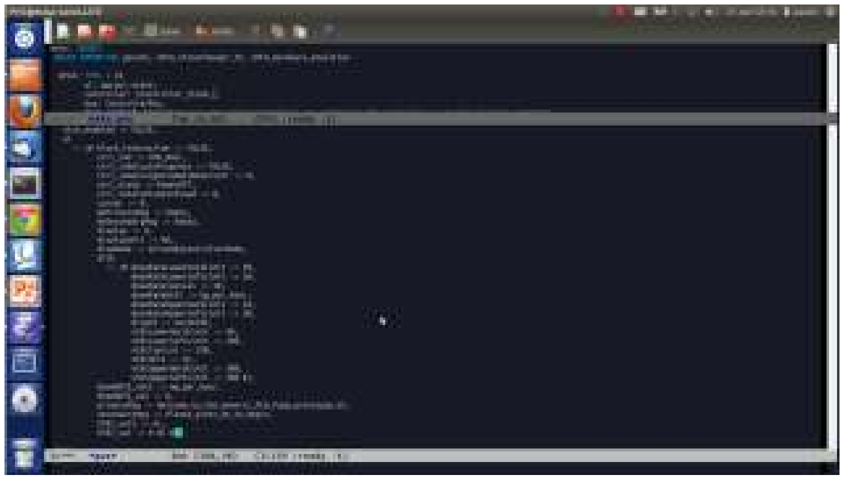
PVSio-web – model-based prototyping in PVS
(www.pvsioweb.org)



Javascript front-end
(defines graphical layout + captures user actions)

User action
(PVS expression)

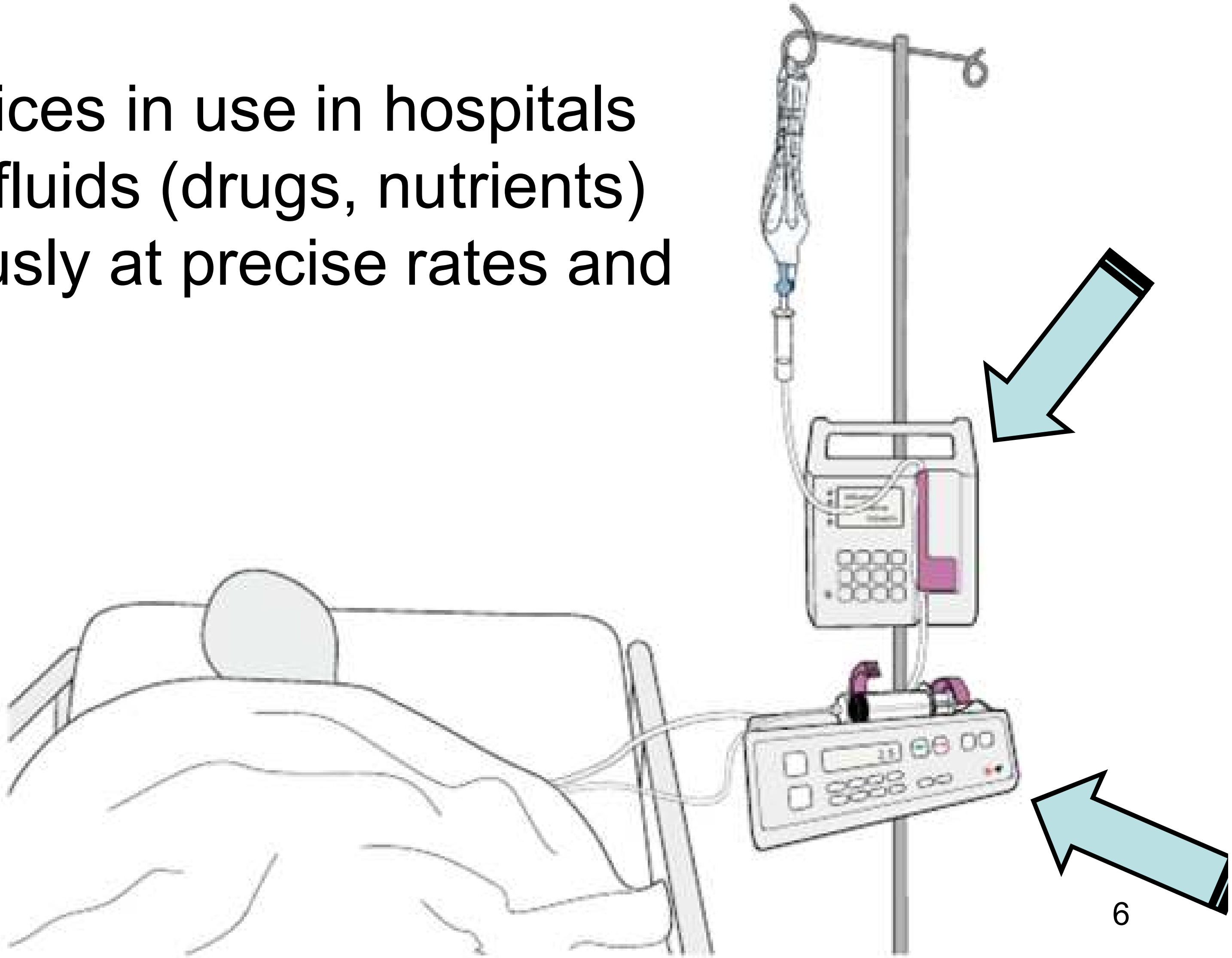
Device response
(evaluated PVS expression)



PVS back-end
(defines the behaviour of the modelled device)

Infusion pumps

Medical devices in use in hospitals to deliver fluids (drugs, nutrients) intravenously at precise rates and volumes.



Queen Mary University of London

chi+med making medical devices safer

Device recalls

Nearly 2,000,000 defective devices recalled in the last decade

- A recall is the removal or correction of a marketed product that regulators consider unsafe (e.g., due to several reported incidents)

Main causes of recalls

- Software defects
- User interface issues

Problems affect all manufacturers and all device models

- Regulators concluded that issues are in the engineering process

Software defects in infusion pumps

Coding bugs

- null pointers, invalid array index, …

Interaction logic bugs

Our approach identifies these bugs

- unexpected device modes
- incorrect feedback
- inconsistent response to user inputs
- …

Examples of interaction logic bugs

Interaction logic
(as explained in the user manual)

- In the Main Menu, open the rate with ◀ and set it with ⁘.

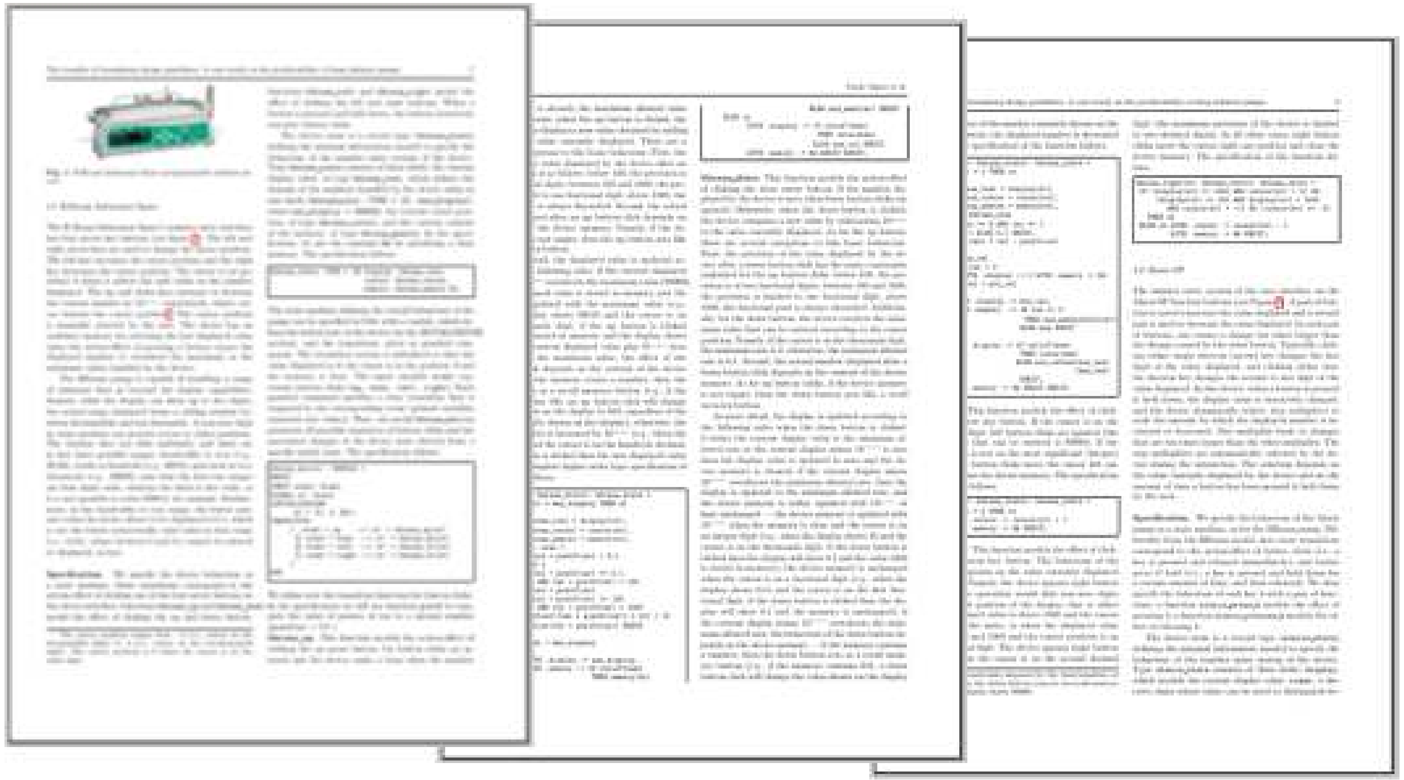
(from the user manual)

Queen Mary University of London

chi+med making medical devices safer

An accurate specification of the interaction logic

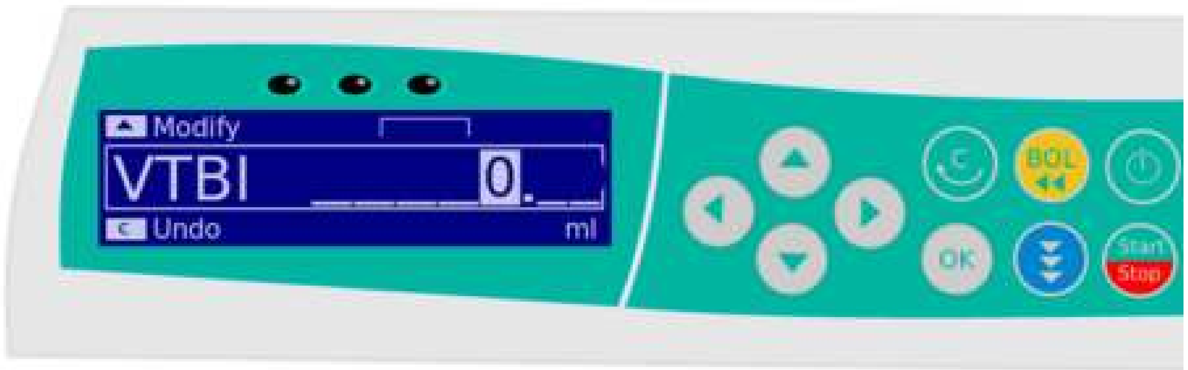
Obtained in our labs by reverse-engineering the real device



Ref: "A case study on the predictability of drug infusion pumps", P. Masci et al,
in Innovations in Systems and Software Engineering, Springer-Verlag London, 2013

Subtle differences in interaction logic

Pump 1



Pump 2

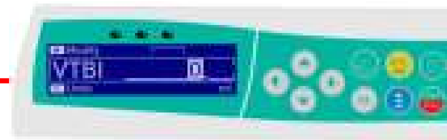
Queen Mary University of London

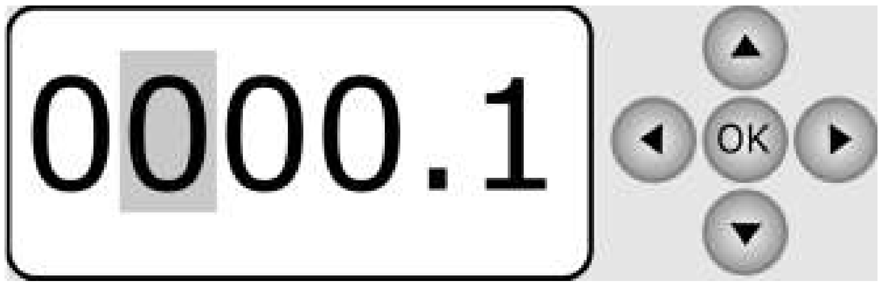
chi+med making medical devices safer

Example task: enter 950mL volume

Key presses: ◀ ▲ (x5) ◀ ▼

Result of key presses on Pump 1





Result of key presses on Pump 2

Ignored key presses

Decimal point erroneously ignored

The key sequence

1	0	0	.	1

is registered as 1001

Devices from different manufacturers have similar problems

The key sequence

1 **0** **0** **.** **1**

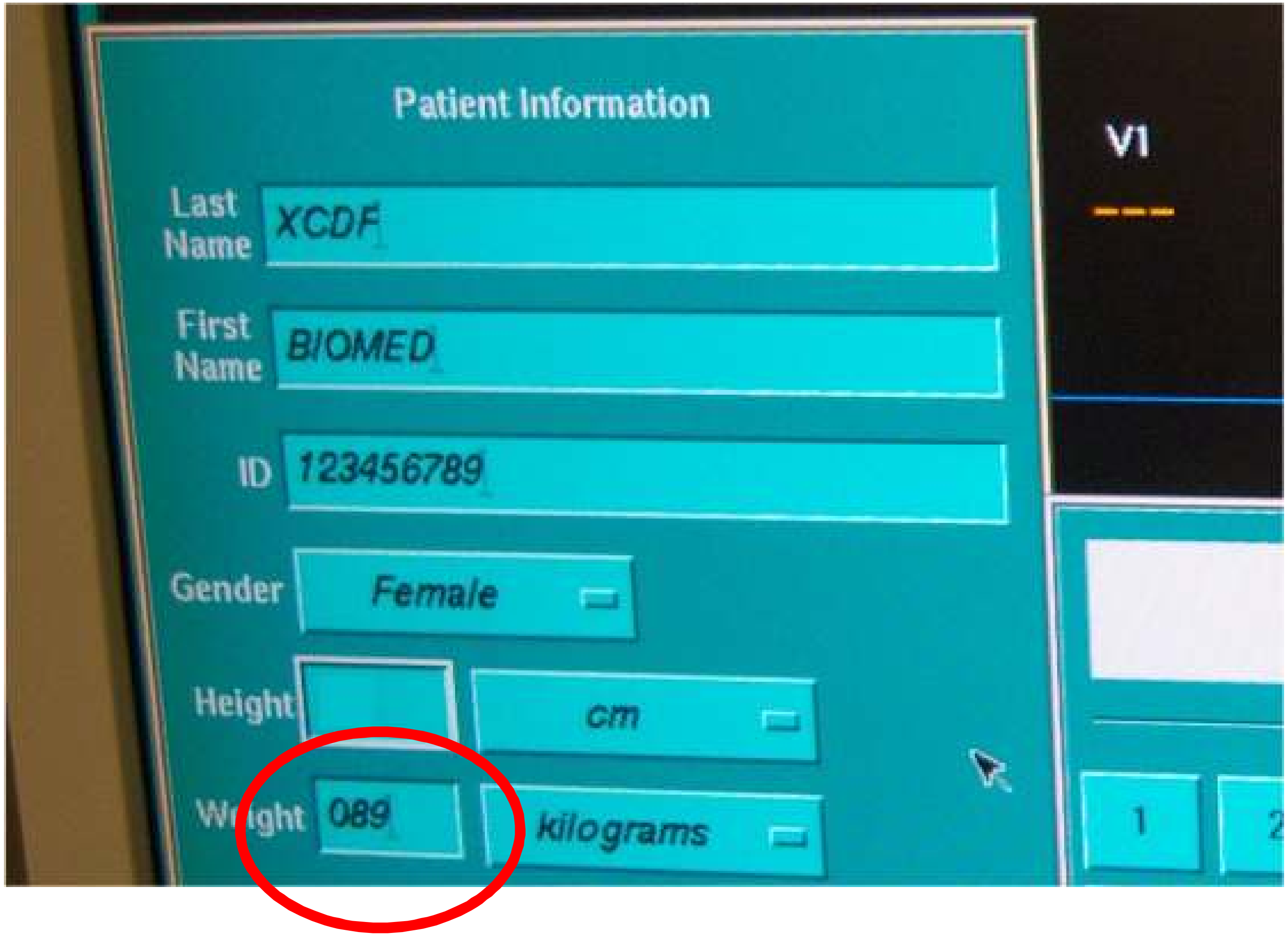
is registered as 1001

(the value is fortunately rejected in this device because the pump configuration limits the rate value to 999 mL per hr)

ill-formed values

Integer values with leading zeros
(they might be easily misread as fractional values)

Patient monitors have similar problems



Discarded values

Discarded values

Entered values are <u>discarded without any warning</u> when input not terminated with "OK"

Queen Mary University of London

chi+med making medical devices safer

Ventilators have the same problem

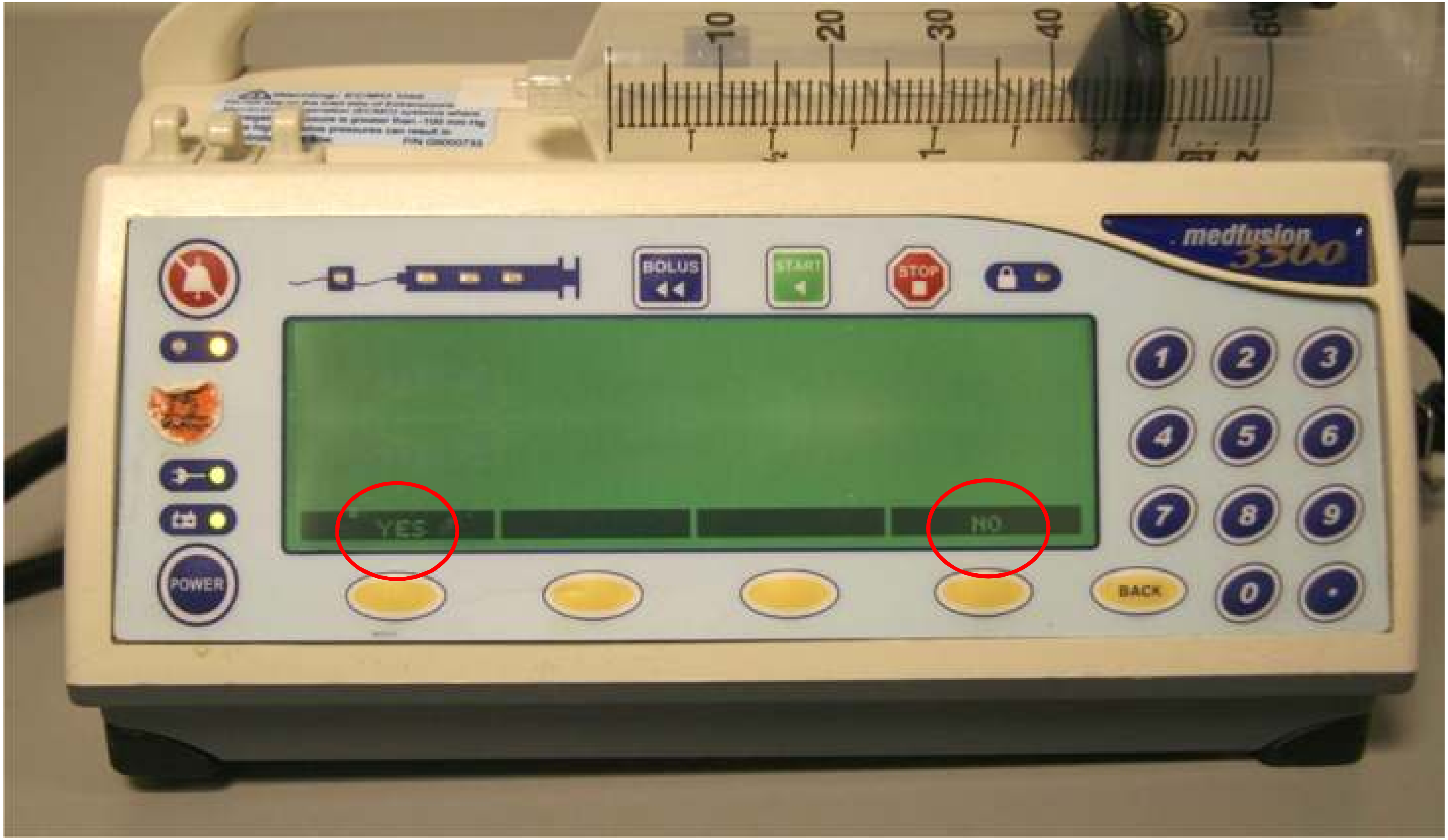
Datex-Ohmeda

Mindray

Draeger Apollo Infinity

Wrong feedback / Non-informative


CareFusion
Alaris PC
Guardrails
A BD Plastipak 10 mL
PRIMARY INFUSION
RATE
0.02 mL/h
VTBI
2 mL
Time Left: < 1 minute
-0.1 is less than MIN RATE
0.1
VOLUME
DURATION
SILENCE
OPTIONS
SYSTEM
ON
Alaris PCA
RATE (mL/h)
CHANNEL
SELECT
PAUSE
CHANNEL
OFF
RESTART
STANDBY


10
20
30
40
medfusion 3500
BOLUS
START
STOP
YES
NO
1
2
3
4
5
6
7
8
9
0
POWER
BACK

Lessons learned

Existing formal tools are effective for the analysis of user interfaces

- We don’t need new formal tools for the analysis of user interfaces, but new front-ends for existing tools!

Model-based prototyping allowed us to engage with key stakeholders

- Clinicians
- Medical device trainers
- Regulators
- Engineers

Key references

“Formal Verification of Medical Device User Interfaces Using PVS.”
P. Masci, Y. Zhang, P. Jones, P. Curzon, H. Thimbleby
In **ETAPS/FASE2014**, Grenoble, France, April 5 -- 13, 2014

“**Model-based development of the Generic PCA infusion pump**”,
P Masci, A. Ayoub, P. Curzon, I. Lee, O. Sokolsky, H. Thimbleby
in **SAFECOMP2013**, , Intl. Conference on Computer Safety, Reliability and Security, 2013

“**Verification of interactive software for medical devices**”
P Masci, A. Ayoub, P. Curzon, M.D. Harrison, I. Lee, H. Thimbleby
in **EICS2013**, ACM SIGCHI Symposium on Engineering Interactive Systems, 2013

“PVSio-web: a tool for rapid prototyping device user interfaces in PVS”
P. Oladimeji, P. Masci, P. Curzon, H. Thinbleby
in FMIS2013, 5th workshop on Formal Methods for Interactive Systems
http://www.pvsioweb.org

Paolo Masci o **Patrick Oladimeji**
(paolo.masci@eecs.qmul.ac.uk) (p.oladimeji@swansea.ac.uk)